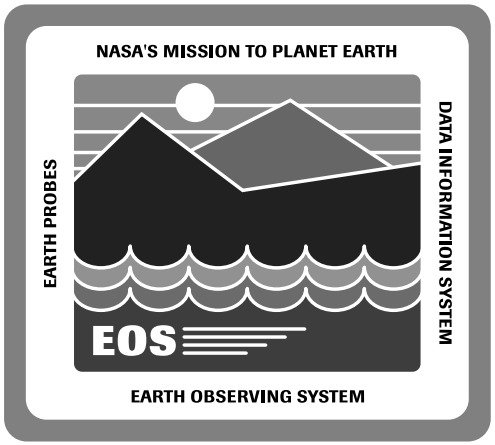


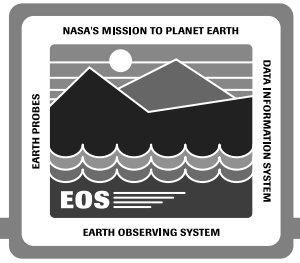

# ECS Security Architecture

## Paul W. Fingerman

**pfingerm@eos.hitc.com**

**ECS Release A SDPS/CSMS Critical Design Review**
**17 August 1995**

# Roadmap




**Why Security?**

**Security Threats and Countermeasures**

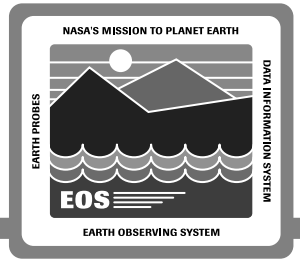
**General ECS Approach to Security**

**Using DCE/OODCE for ECS Security**

**Gateway Architecture**

**Summary**

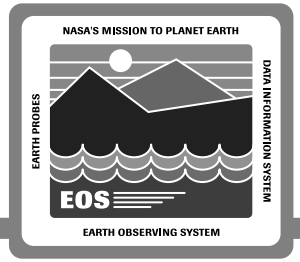
# Why Security?




**To maintain three characteristics**

- **Integrity of ECS (e.g., data products, production schedules)**
- **Availability of ECS services**
- **Confidentiality of certain data (e.g., user request logs)**

# Security Threats




**Intentional Acts**

- **Unauthorized alteration**
  - **Malicious insertion**
- **Unauthorized use**
- **Unauthorized disclosure**
- **Sabotage, external**
- **Sabotage, internal**
- **Industrial espionage**

**Modes of Attack**

- **Impersonation**
  - **Hijacking (devices, sessions, authenticators)**
  - **IP spoofing**
- **Denial of service**

**Accidents**

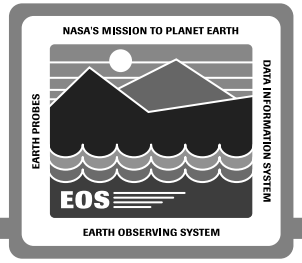
- **Programming error**
- **User error**
- **Inadvertent disclosure**
- **Software malfunction**

# Security Countermeasures

**Combination of physical security, technical security, and administrative security**

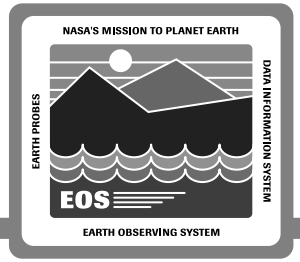
- **Physical Barriers or Operational Procedures**
  - **Access to devices**
  - **Network access**
- **Administrative Barriers**
  - **Software quality controls**
  - **Management of physical and technical barriers**
  - **Audits and alerts**

# Security Countermeasures (Cont)




| | Subsystem | | | |
|---|---|---|---|---|
| **Form of Security** | **ISS** | **CSS** | **MSS** | **Application** |
| ***Routing Control*** | | | | |
| **Address Filtering** | √ | | √ | |
| **Dual Homing** | √ | | | |
| **Firewalls** | √ | √ | √ | √ |
| ***Authentication/Authorization Exchange*** | | | | |
| **DCE** | | √ | √ | √ |
| **Raw Kerberos** | | √ | √ | √ |
| **Other (weak)** | | √ | √ | √ |
| ***Access Control*** | | | | |
| **DCE ACL Mgr** | | √ | √ | |
| **App. Rules** | | | √ | √ |
| **Gateway Rules** | | √ | √ | √ |
| ***Data Integrity*** | | | | |
| **Encrypted Checksums** | √ | √ | | √ |
| ***Data Privacy*** | | | | |
| **DCE Encryption** | | √ | | |
| ***Administrative Procedures*** | | | | |
| **Audit Trails** | | | √ | |
| **Logoff/Timeout** | | | √ | |
| **[DAAC Autonomy]** | | √ | √ | |
| ***Physical Measures*** | | | | |
| **Facility Access** | √ | | | |
| **Distinct Servers for BBS** | √ | √ | √ | |
| **Replication** | | √ | √ | |
| **ISOLans** | √ | | √ | |
| **[ISOCells]** | | √ | √ | |

# General ECS Security Approach



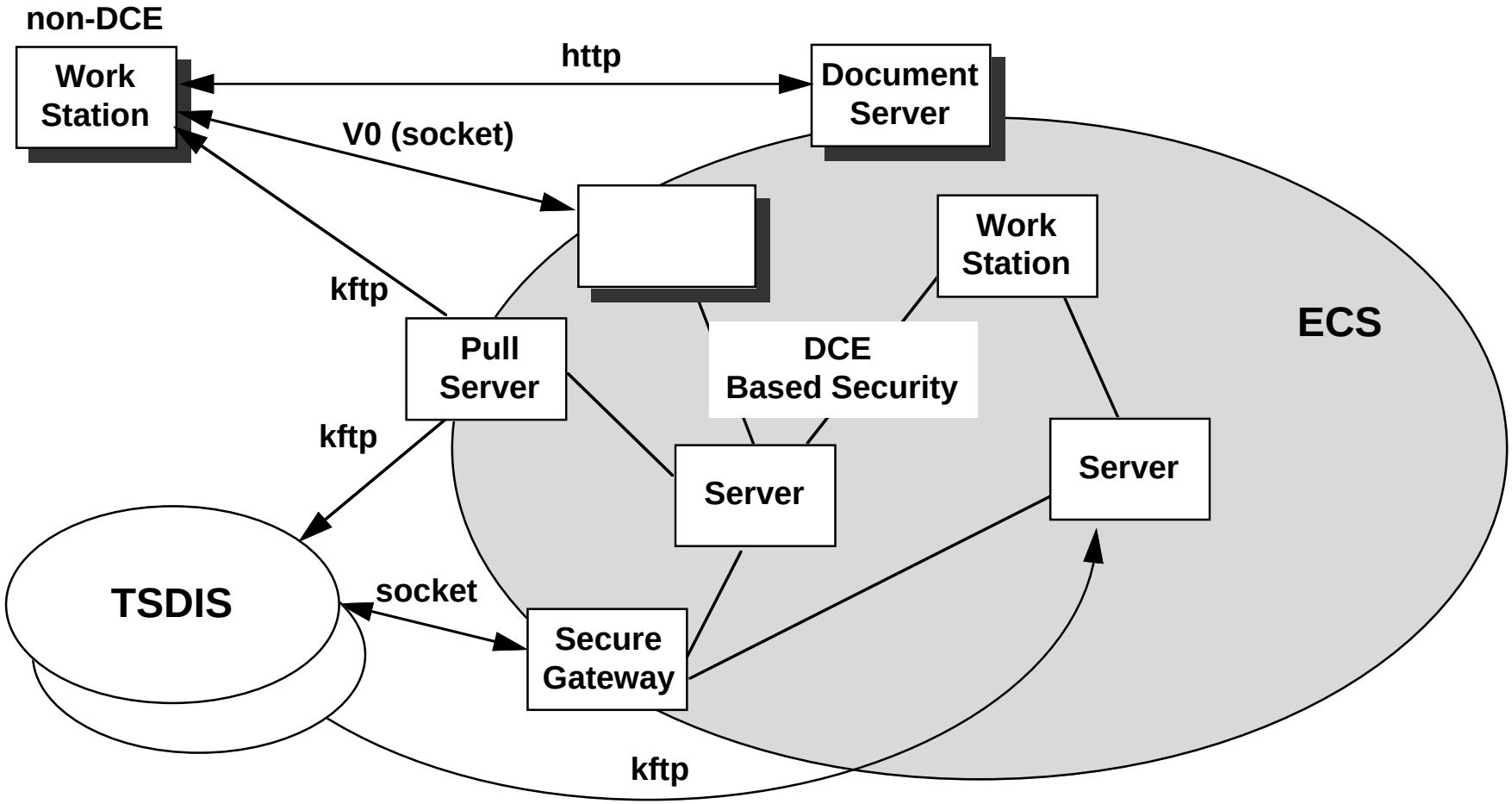

**Use OSF/DCE & OODCE as the core for information security for ECS**

- **Inside the ECS DAAC**
- **Internal clients at Release A**
- **External clients at Releases B and beyond**

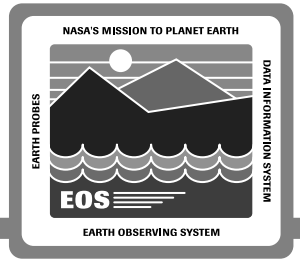
**For external ECS interfaces and legacy systems (V0, TSDIS) that will not have DCE/OODCE**

- **Attempt, in so far as possible, to be policy-neutral or policy-flexible**
- **A security gateway has been added to the architecture**
  - **Kerberos will be supported as an alternative**

# General ECS Security Approach (Cont)

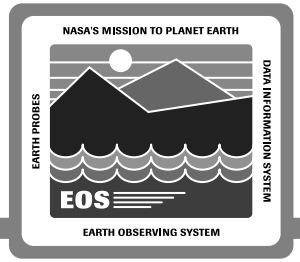


# DCE/OODCE Security Capabilities




- **Authentication**
  - **Verifying the identity of the principal**
  - **Establishing affinity to a group/organization**
- **Privilege Attribute Certificate (PAC)**
  - **Trusted mechanism for conveying client authorization data to authenticated servers**
- **Access Control List (ACL)**
  - **List of access control entries that protects an object**
- **ACL Manager type**
  - **Creates and manages ACL databases**
  - **Defines access control permissions**
  - **Creates and associates ACLs to objects**
  - **Supports standard interfaces for external systems**
- **Authorization using Access Control Lists (ACLs)**
  - **Checking the privileges of a principal using PAC (Privilege Attribute Certificate)**

# Using DCE Cells To Provide Additional Security

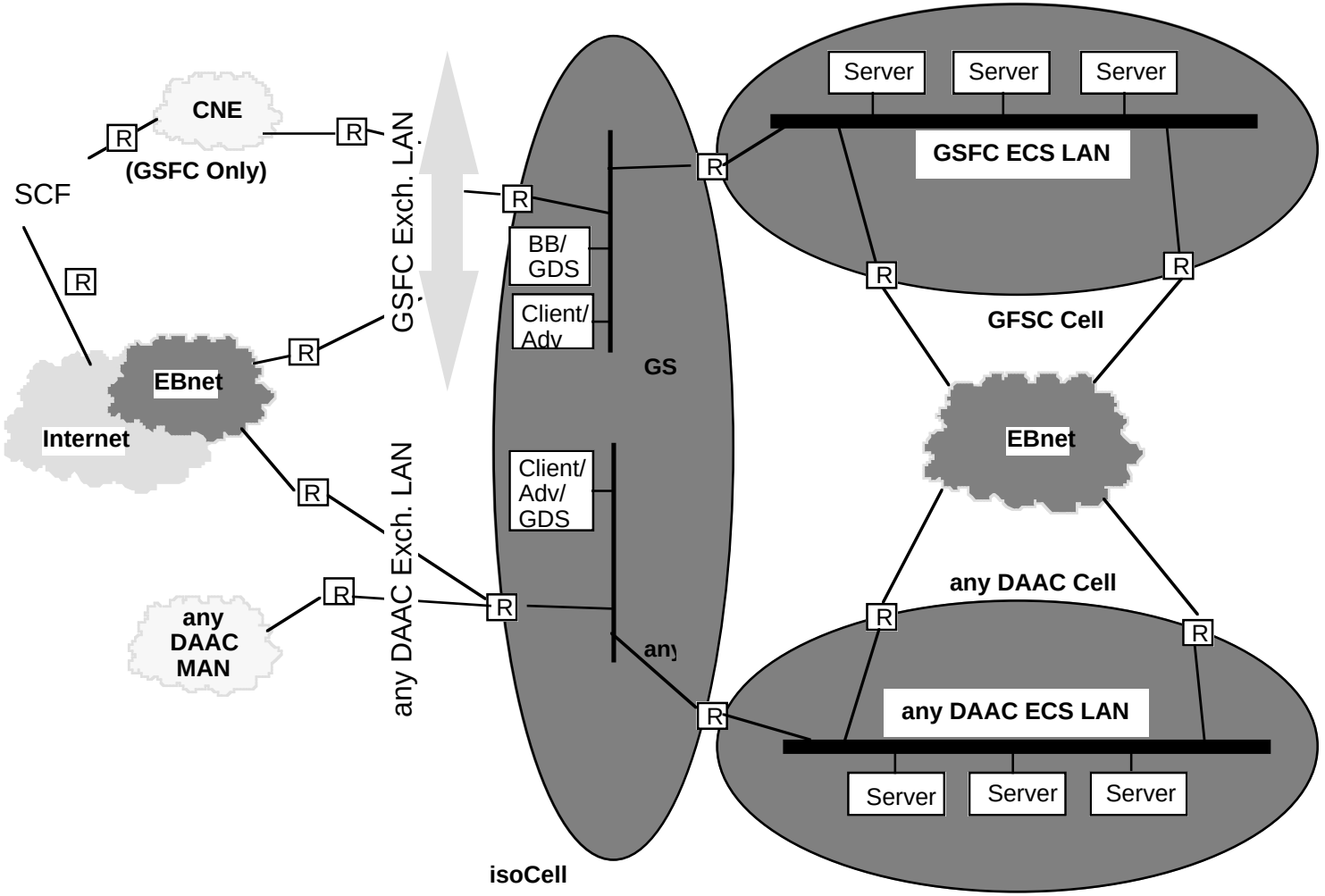



- DCE provides “cells”
  - Can be used to provide security
  - One cell per DAAC
  - One (or more) ISO cell containing gateways for external/guest users
  - Users in one cell could access services in another by cross-cell authentication

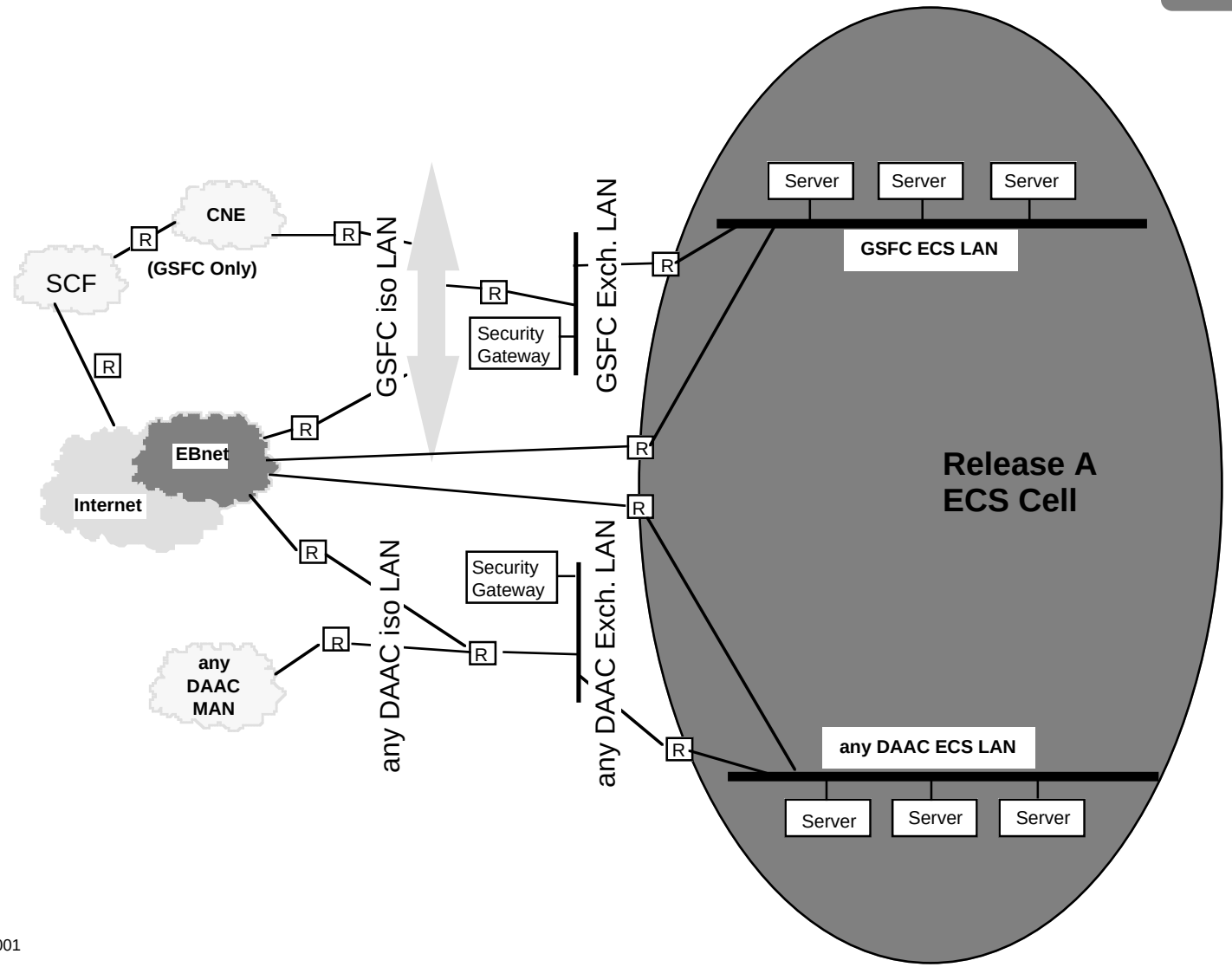
- Release A uses a single-cell architecture
  - OSF/DCE 1.0.3 currently available from vendors does not support all requirements for Release A
  - OODCE currently does not provide cross-cell authorization

- Will transition to multi-cell architecture for Release B

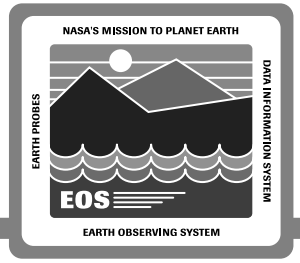
# Using Multiple DCE Cells To Provide Additional Security



# DCE Single-Cell Architecture for ECS Security at Release A



# Generic Gateway Architecture




**Gateway Components**

- **Communications Gateway**
  - **Performs transport layer conversion (TCP sockets to OODCE-based distributed objects)**

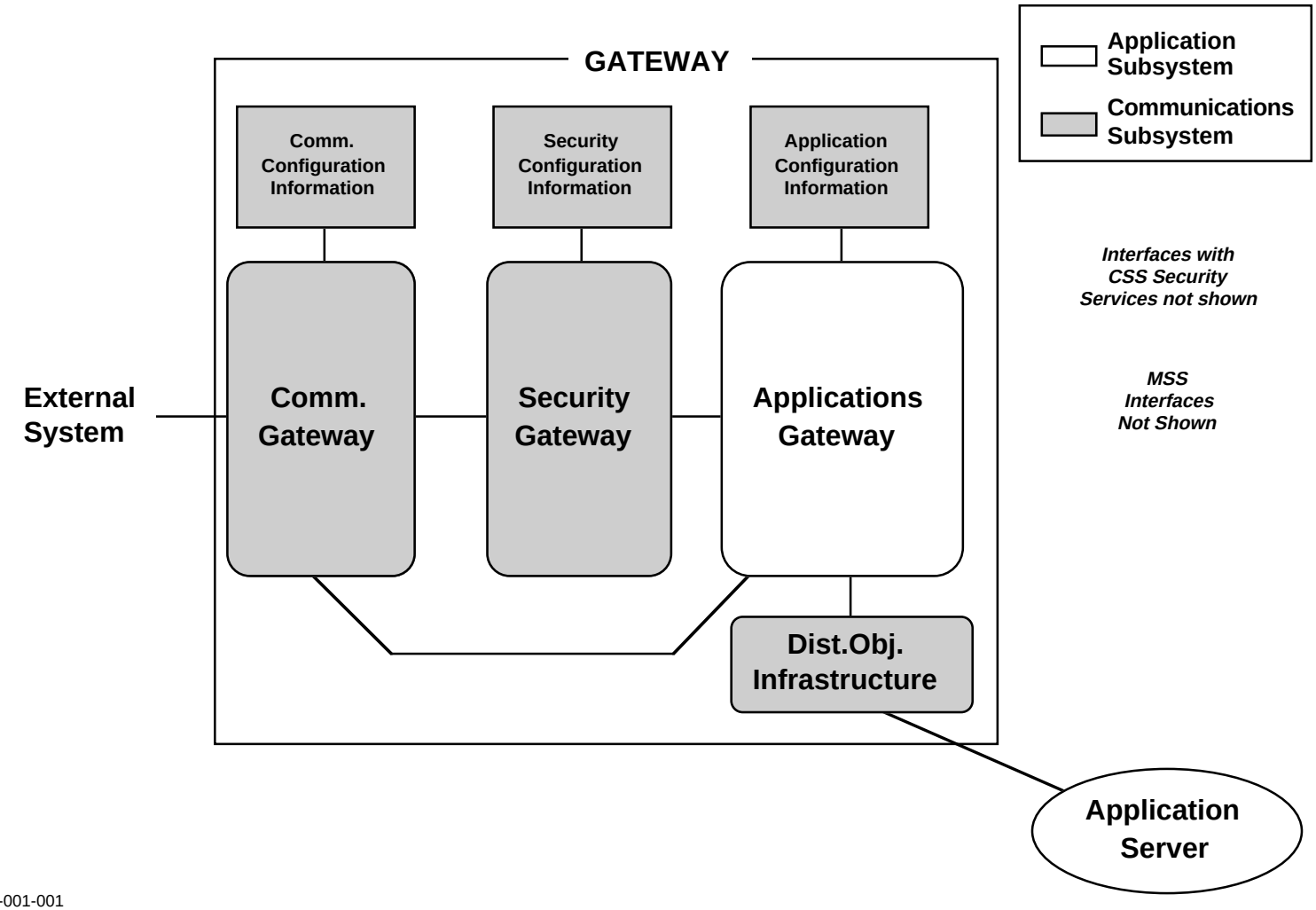
- **Security Gateway**
  - **Performs security protocol conversion (e.g. Kerberos-authenticated to DCE-secured RPCs, V0 authenticated to DCE)**
  - **Enforces security barrier**

    **Authorization constraints (per policy)**

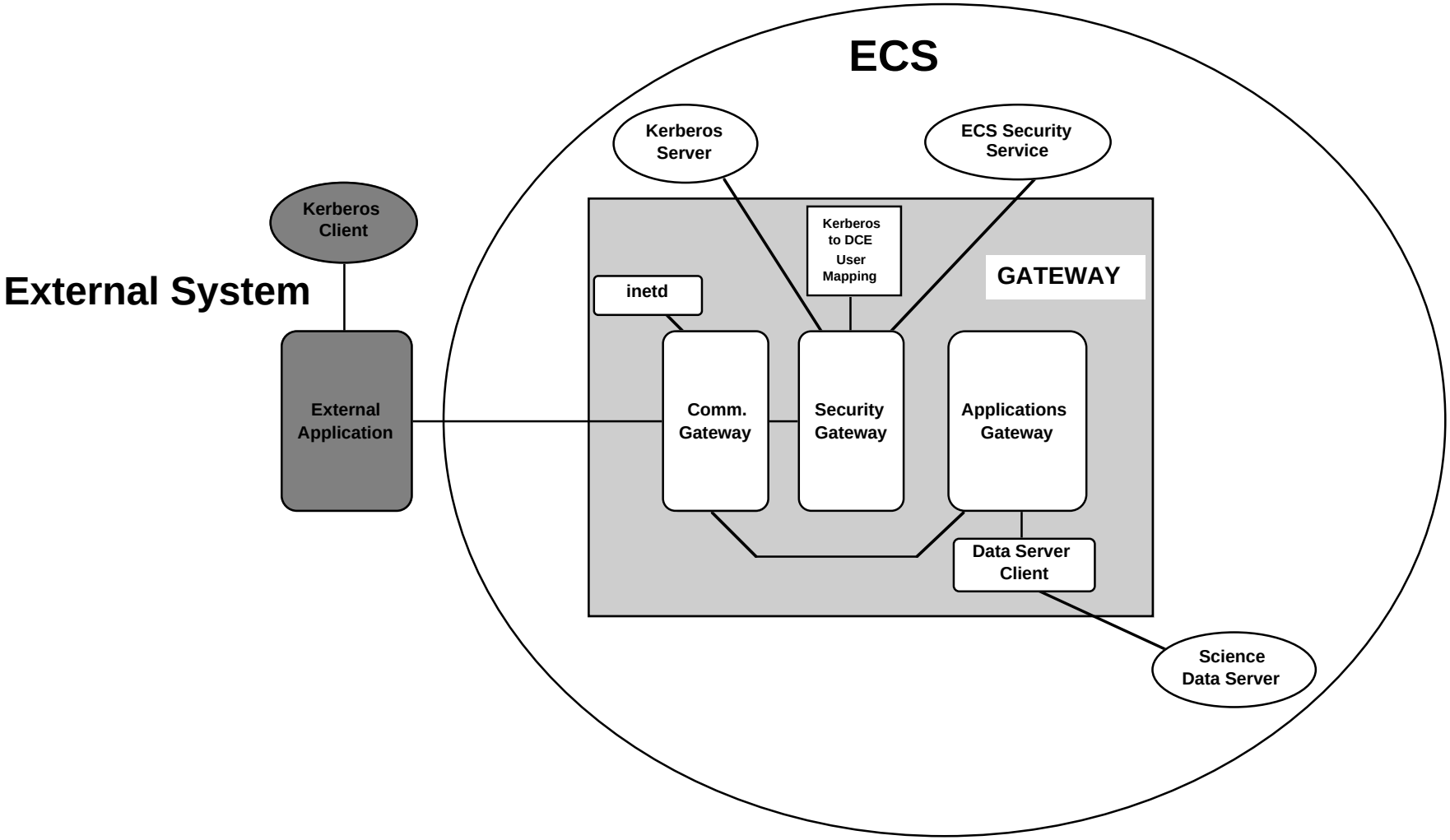
- **Application Gateway**
  - **Parses and interprets incoming requests**
  - **Converts application layer protocol, e.g., Object Description Language (ODL)-to-Distributed Object Framework (DOF)**

**Bulk data transfers bypass gateway after authentication**

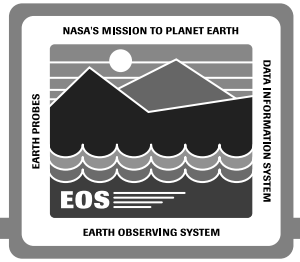
# Generic Gateway Architecture (Cont)



# Kerberos Gateway Architecture Example



# Summary




**Most external clients will not use DCE**

- **Architecture now provides for Security Gateway**

**DCE provides internal security solution for ECS**

- **Single-cell architecture for Release A**
- **Transition to multi-cell architecture by Release B**

**We have an "Enterprise-wide, integrated security concept, design, and baseline implementation plan" that**

- **Provides common, flexible security structures**
- **Promotes consistent placement of security functions & services**
- **Allows for a variety of security policies at external interfaces**